N CSC-EPL-87/006

2

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT OF MICRONYX, INC. TRIAD PLUS

VERSION 1.3

31 August 1987

SUB-SYSTEM EVALUATION REPORT

MICRONYX, INC.

TRIAD PLUS VERSION 1.3

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

August 14, 1987

CSC-EPL-87/006
Library No. S228,557

FOREWORD

This publication, the Sub-system Evaluation Report, Micronyx, Inc., Triad Plus version 1.3, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the evaluation of Micronyx's Triad Plus. The requirements stated in this report are taken from Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985.

Approved:

August 14, 1987

Eliot Sohmer
Chief, Product Evaluations and Technical Guidelines,
National Computer Security Center

ACKNOWLEDGEMENTS

Evaluation Team Members

James L. Arnold

Stephen F. Carlton

Shawn M. Rovansek

John W. Taylor

National Computer Security Center
9800 Savage Road
Fort George G. Meade, Maryland 20755-6000

CONTENTS

This page intentionally left blank.

EXECUTIVE SUMMARY

Triad Plus(1) version 1.3 has been evaluated by the National Computer Security Center (NCSC). Triad Plus is considered to be a security sub-system rather than a complete trusted computer system. Therefore, it was evaluated against a relevant subset of the requirements in the Department of Defense Trusted Computer System Evaluation Criteria (TCSEC), dated December 1985. Specifically, the features included in this evaluation were Identification and Authentication (I&A), Discretionary Access Control (DAC), Object Reuse, and Audit. In addition to DAC on objects, Triad Plus was found to implement a technology which provides DAC on all devices and communications ports. This feature is referred to as Resource Access Control (RAC) throughout this report.

The NCSC evaluation team has determined that Triad Plus is capable of applying these security features to any IBM PC/AT or PC XT(2) configured as tested. Triad Plus maintains user I&A by requiring that users identify themselves and provide authentication before gaining access. DAC is provided on individual user's files through the use of file descriptors and, for further assurance, encryption. The RAC mechanism provides the capability to control the access that individual users have to the various resources of the system (i.e., hard disk, floppy drive, printer port, etc.). By over-writing files that have been deleted, the object reuse mechanism gives assurance that data can not be scavenged. In addition, Triad Plus provides the means to audit workstation activity, including attempts to violate the security of the system.

The security mechanisms provided can only be trusted if the code which implements them is protected from modification. This protection is difficult to implement in a computer system which only provides a single state of execution (e.g., a PC). However, Triad Plus is able to maintain its own state of execution through

[1] Triad Plus is a registered trademark of the Micronyx Corporation.

[2] IBM PC/AT and PC/XT are registered trademarks of the IBM Corporation.

the use of a memory management scheme known as the Controlled Access Mechanism (CAM)[1]. Thus, it is able to protect the security mechanisms it provides.

[1] Controlled Access Mechanism (CAM) is a registered trademark of the Micronyx Corporation.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems: systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry- and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Sub-system Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the TCSEC. The NCSC has, therefore, established a Computer Security Sub-system Evaluation Program.

The goal of the NCSC's Computer Security Sub-system Evaluation Program is to provide computer installation managers with information on sub-systems that would be helpful in providing immediate computer security improvements to existing installations.

Introduction

Sub systems considered in the program are special-purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security sub system evaluation is limited to consideration of the sub system itself, and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an attempt is made, where appropriate, to assess a sub system's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

Triad Plus is an add-on security product which, when implemented on any IBM PC XT or PC/AT, configured as tested, provides user Identification and Authentication (I&A), Discretionary Access Control (DAC) on objects, DAC on system resources (RAC), Object Reuse, and Audit mechanisms. Once a user has logged on to the workstation, these mechanisms are essentially transparent. Unless the user attempts to exceed his defined privileges, the only noticeable difference is a slight degradation in workstation performance.

Triad Plus is comprised of an expansion board, personal identification tokens, and supporting software utilities. The expansion board itself provides all of the security mechanisms. The I&A mechanism is used in conjunction with a personal identification token. A token is a key encoded with security relevant information. The token must be inserted into the token receptacle connected to the Triad Plus board in order to log on to the workstation. The software utilities provide the ability to alter the specific characteristics of the security mechanisms. For example, the ownership utility is used to control the ownership of newly created files. In addition, a manager program is provided to access the Triad Plus configuration data such as user profiles and general system security parameters. Of the complete list of utility functions provided, a select few are privileged; only a user of the administrator group may execute them. The privileged commands consist primarily of the manager program, functions relating to audit record access, and overriding Triad Plus security mechanisms.

The Triad Plus system provides for one primary administrator and any number of secondary administrators. There must always be a primary administrator defined on the system. Administrative privilege is delegated to the secondary administrators from any other administrator by defining the new administrator to be in the 'Administrator' group. The difference between the primary and secondary administrators is that the primary administrator is the only user, including administrators, who can alter his profile. Thus, the primary administrator cannot have his privilege revoked by anyone other than himself.

In addition to the security features listed above, Triad Plus uses an intricate memory management scheme, referred to as the Controlled Access Mechanism (CAM), to protect the resources on its expansion board. The CAM disallows random access to the information on the board by only allowing access through specific controlled entry points within the workstation's address space.

Evaluation of Functionality

The team has determined that Triad Plus provides mechanisms for I&A. DAC. RAC. Object Reuse. and the Audit of workstation activity. Each is described separately below.

Identification and Authentication

In order to access a machine on which Triad Plus has been installed a user must first pass through the I&A mechanism. After the workstation has been powered on or reset. a logon window appears which prompts the user for his primary identifier. This identifier has been previously assigned by the Workstation Administrator (WA). After entering the identifier. the user may be prompted for a secondary identifier and/or project identifier if the WA has configured the system to require either one or both. Next. the user is required to insert his token into one of the slots in the token receptacle connected to the workstation. A 'jingle sound will be heard when the token has been inserted properly. Now the user is prompted for his password which is not displayed when being typed in.

If the primary identifier. secondary identifier. password. or token data does not match the user's profile. access is denied without revealing the reason. After multiple logon failures. all logon attempts are suspended during a predetermined logon lockout period. Successive logon failures invoke both a logon lockout and a logon alarm. The lockout and alarm times are defined by the WA.

If the logon entries are correct. user access is subject to logon time zones that have been defined by the WA. Each user can be allowed to logon during any of four time zones specified as hours of the day and days of the week.

Triad Plus can be configured to enforce password updates based on a minimum and maximum password lifetime defined by the WA. When a password is updated. it is subject to a WA configurable minimum password length. and it must be different than the previous password.

Suspend, an additional feature of I&A is also provided. It protects the user's information without requiring an exit from the current application. This feature is automatically invoked after a fixed period of workstation inactivity, set by the WA, or by explicit user action (i.e., suspend command or user-definable suspend keys). Upon invocation, the workstation screen is cleared, a 'Suspend' message is displayed, and the workstation is disabled. When any key is pressed, a logon window appears and the user must go through the same procedure as an initial logon. However, only the user who is suspended can be authenticated. All other users must reset the workstation, thereby causing the suspended user to be logged off. When a suspended session is restored by the appropriate user, the interrupted application is restored to the point at which it was suspended.

Discretionary Access Control

Triad Plus provides DAC on individual files by allowing the creating user to specify who may access them. A user controls access to files by using the OWNER command followed by the attributes that the file is to be given. Attributes include ME, GROUP, MACHINE, COMPANY, and PUBLIC. The files are protected using encryption(1) and file descriptors, based on the chosen attribute. The ME attribute protects files based on a user's primary identifier. Only that user can access the files. The GROUP attribute controls access based on the users secondary identifier. All user's with the same secondary identifier may access these files. The MACHINE attribute protects files based on a unique key given to each individual workstation by the WA. A file protected with this attribute can only be accessed on the machine on which it was created. The COMPANY attribute protects files based on a special configuration name assigned by the WA. Any file protected with this attribute may be accessed on any workstation with the same configuration name. The last attribute, PUBLIC, allows anyone to access the file. This is the default attribute, and all files with this attribute are unprotected and are not encrypted.

(1) The encryption is provided by a SmartCypher encryption circuit. SmartCypher is a registered trademark of Micronyx, Inc.

Another feature of DAC is the ability to hide inaccessible files. This feature is an option that can be set by the WA. When it is set for file hiding, a file that is inaccessible to the user based on ownership attributes is hidden from all DOS references to the file.

Resource Access Control

Triad Plus provides the capability to control the resources available to the workstation. Up to eight enumerated access states can be defined by the WA. Each access state is a list of devices, along with the corresponding type of access (i.e., read or read write), that a user defined with that state may use. Each user is assigned one of these access states by the WA during configuration. By default a user can only access those devices listed in his assigned state, however the WA may configure the system so that the user would also have access to any devices listed in any logically lower states. This feature is referred to as Mandatory Access Control (MAC) in the Triad Plus documentation. In this report, the feature will be referred to as RAC in order to avoid confusion with MAC as described in the TCSEC. Conceptually, RAC is a limited implementation of DAC on devices. There are thirteen devices and communication ports in the Triad Plus access control list. They include diskette read, diskette read write, hard disk 0 read, hard disk 0 read/write, hard disk 1 read, hard disk 1 read write, parallel printer adapter, asynchroncus adapters, binary synchronous communications adapters, synchronous data link control adapter, network communications adapters, Digital Communications Associates IRMA card, and ARCNET cards.

Object Reuse

Triad Plus provides two types of Object Reuse. First, every time a user logs off, all user memory is overwritten. This prevents a user from leaving behind any programs or data that could compromise security. Second, Triad Plus may be configured by the WA such that when a file is removed by DOS, the disk sectors of the deleted file are overwritten. Normally, when a file is deleted under DOS, the contents of the file remain on the disk and may be recovered by certain utility programs. This option prevents that from occurring. When this option is set by the WA, file overwrites are automatic and transparent to the user when a file is deleted either by explicit user action or by application programs using DOS calls to delete files.

Audit

Triad Plus provides the capability to create an audit trail of workstation activity. Events that are recorded are logon, logoff, logon failure, project registration, PC-DOS program execution, session suspend, failure to end suspend, I/O access violations, file access violations, and session summary. The audit trail for each user session contains the date and time of each event, the primary and secondary user identifier associated with the session, the access level of the user, the configuration identifier, the machine identifier, the project identifier, and the type of each event. The audit trail exists in a secure RAM buffer and will hold the last 100 to 200 audit records. Triad Plus can be configured to automatically send the audit records to a specified file when the secure buffer fills up.

Evaluation of Documentation

The Micronyx Triad Plus documentation consists of two guides, the Workstation Administrator's Guide, 1987, version 1.0, and the User's Guide, 1987, version 1.0. These two documents, described below, contain a detailed description of the security features provided by Triad Plus. The documentation assumes a minimal knowledge of computers.

Workstation Administrator's Guide

This manual is intended for the individual responsible for installing the system and also for the WA. The following sections are included:

Introduction

The introduction lists the components of the Triad Plus sub-system and the hardware and software base required to use it.

Chapter 1: About Triad Plus

This section describes the role of Triad Plus in providing a more trusted environment for the user's computing needs. It also explains some basic security concepts and how they are implemented by Triad Plus.

Chapter 2: A Technical Overview Of Triad Plus

The technical dimensions of Triad Plus are covered in this section. These include the products supported by Triad Plus, as well as the features provided by it (i.e., I&A, DAC, RAC, Object Reuse, and Audit).

Chapter 3: Installing Triad Plus

This section provides a detailed explanation of the Triad Plus installation process.

Chapter 4: Manager: The Configuration Utility Program

Usage of the Workstation Manager Utility Program is detailed in this section.

Chapter 5: Workstation Access Control

This section provides information on administrator-defined access controls. These controls include: logon availability periods, duration of lockout and alarm periods enforced on successive failed logon attempts, password update requirements, accessible peripherals, and required identifiers and passwords.

Chapter 6: Defining Users And Their Privileges

This section explains how to grant access privileges to users. It includes information on fields to be defined, programming tokens, and changing previously defined user information.

Chapter 7: File Protection And Auditing

This section provides descriptions of the Audit, Object Reuse, and DAC mechanisms.

Chapter 8: User and Privileged Commands

This section provides a summary of the commands and their respective parameters available with Triad Plus. The privileged commands are differentiated from the general user commands and examples of all commands are provided.

Chapter 9: Simplifying Things For The User

The procedure to be followed, during installation of Triad Plus, in order to establish automatic initiation of application programs is covered in this section.

Appendix A: The ABC Company

This section describes the ABC Company. The ABC Company is a fictional company used in the manual to illustrate the role of Triad Plus in meeting the security requirements of a typical firm.

User's Guide

This manual is intended for the Triad Plus general user (e.g.. one without WA privileges). It provides instruction on basic usage of the product and tends to overlap with the Workstation Administrator's Guide in this area.

Introduction

The introduction summarizes the capabilities of Triad Plus and introduces the user to *some of the security concepts* that the product implements.

Chapter 1: Logging On

This section shows the user how to log on. It presents an explanation of the product's possible responses to a logon attempt.

Chapter 2: What Is A Guest User?

This section explains how a user without defined access to a workstation may still use it to perform tasks that do not require the use of protected files and resources.

Chapter 3: Triad Plus User Commands

The Triad Plus commands that a general user may utilize are detailed in this section. These commands allow a user to set up the working environment, change project registration, import and export protected files from other workstations, control the file access process, and gain information about protected files in storage.

Chapter 4: Triad Plus And Your System

This section provides suggestions on how to use the commands described in the previous chapter to simplify interaction with Triad Plus.

Chapter 5: When Things Go Wrong

This section presents what the designers feel will be the most common problems that users will have with the product and solutions to them. Problems covered include, but are not restricted to: lost tokens, forgotten passwords, file ownership, and non-U.S. English Keyboard Drivers.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The rapid introduction of office automation products into the workplace has brought with it the need to protect and control access to data stored on these systems. Initially, protection was provided solely by the individual who maintained physical possession of his own data and operating system on diskettes, resulting in a reasonably high assurance of maintaining data and code integrity. These procedural controls isolated users, and thus prevented intentional or accidental access to other users' data. Other security mechanisms were not deemed necessary since the user was only able to inflict damage to his own data or operating system.

The advent of inexpensive and reliable hard disk drives introduced new security implications. In a working environment where it was common to have many users share the same workstation, they now shared and stored their data on the same hard disk memory unit. In this environment, users no longer had the assurance that their data was protected from unauthorized access, or even that the underlying operating system had not been subverted. Procedural controls could no longer provide the adequate user isolation and controlled sharing necessary for this environment.

The Micronyx Triad Plus product is designed to help add assurance in the protection of individual users' data on an IBM PC/XT or PC/AT workstation. When configured as tested, Triad Plus provides effective I&A, DAC, RAC, Object Reuse, and Audit mechanisms.

Although implemented on a single-state architecture (e.g., the IBM PC/XT), Triad Plus implements a technology, CAM, to create its own state of execution in order to provide a trusted and unmodifiable reference monitor. In addition to providing its own state of execution, Triad Plus can also detect when it has been physically removed from the workstation. When the board is removed, all configuration data stored on the board is lost. Thereafter, because the system will insist upon being reconfigured, any user will immediately be made aware that something has happened to the Triad Plus hardware.

The Triad Plus security mechanisms are implemented using hardware and interrupt-driven software. The design is such that the product is virtually transparent to the DOS environment; no restrictions are placed on the use of DOS commands. Other than during logons and attempted security breaches, the only noticeable effect of Triad Plus is a slight degradation in performance. This degradation manifests itself in the form of slower response time and occasional conflicts with interrupt-driven applications.

Triad Plus provides an I&A mechanism which requires both a password and a personal identification token to log on. This means that a user must provide information that is known only by that user and Triad Plus. Further, Triad Plus requires physical proof, in the form of the token, of the user's authorization to use the workstation before access is granted.

Once logged on, individual users' files are protected by the Triad Plus DAC mechanism. Although this mechanism can be circumvented by the use of various disk utility programs, any data scavenged in this manner is encrypted. The evaluation team did not examine the encryption algorithm.

The product also provides RAC to control user access to system devices (e.g., floppy disk drive, hard disk drive, printer ports, communication ports). The RAC consists of discretionary read and write privileges for each system device. These privileges are controlled by Triad Plus Administrators. Up to eight enumerated states, optionally hierarchical, of device access can be defined on the workstation. Each user is then assigned one of these RAC states.

In addition to the standard security features, the vendor states in his documentation that Triad Plus works with local area networks, securing both access to the network itself and access to Triad protected files. No attempt was made by the team to evaluate this claim due to the lack of a suitable PC network.

This product implements several features that can be effective in providing trust for a large environment of multiple workstations. The DAC mechanism allows data to be associated with a particular workstation or workstation group, as well as with a particular user or user group. In addition, data encryption allows information to be passed from machine to machine in encrypted form, providing at least some assurance that the information will not be disclosed. The Triad Plus configuration information may be stored on removable media, this allows additional workstations to be configured identically with very little additional time or effort.

PRODUCT TESTING

Test Procedure

Testing represents a significant portion of a sub-system evaluation. The testing performed was primarily functional in nature; the security relevant characteristics of the product were compared against the claims of the vendor. The functional test suite of this product focused upon the following features: I&A, DAC, RAC, Object Reuse, and Audit. These security relevant features were identified in the Workstation Administrator's Guide, version 1.0.

This test suite consisted of several parts. The I&A mechanism was tested extensively, including attempts to subvert it and to bypass it entirely. Object Reuse tests were performed. They consisted of creating and deleting files and searching for remains of the file's contents on the disk media. In addition, memory was scanned after a log off and a new user logged on. The DAC mechanism was subjected to high level access decision testing, involving authorized as well as unauthorized accesses to objects protected by various combinations of the available Triad Plus DAC file descriptors (i.e., user, group, machine, company). The DAC mechanism was also examined at a lower level. Specifically, attempts were made to bypass this mechanism using various disk utility programs. The RAC was tested from the operating system interface and from system utility programs capable of making direct BIOS calls in order to ensure that the resources were adequately protected. The Audit mechanism underwent extensive testing; consisting of attempts to subvert or bypass the mechanism itself, attempts to corrupt audit data, and an attempt to overflow the audit data storage area. Further testing was performed on Triad Plus's CAM in order to determine whether it could protect its own Random Access Memory, which contains information (e.g., user logon profiles) vital to the trusted operation of this product. In addition, some limited testing was conducted using the XENIX(1), version 1.0, operating system on an IBM PC/AT(2).

[1] XENIX is a registered trademark of MicroSoft Corporation.

[2] The IBM PC/AT was configured with a single floppy disk drive and a single fixed hard disk drive.

Product Testing

All tests, unless noted otherwise, were performed on both an IBM PC/AT(1) and IBM PC/XT(2) operating under the PC-DOS(3) versions 3.1 and 3.2.

Test Results

The test results described below are basically oriented towards providing the evaluation team's opinions concerning the strengths and weaknesses of each security relevant feature provided by Triad Plus.

Identification and Authentication

The I&A mechanism was found to function properly; no access was granted to the machine prior to entering all requested I&A information. The information used by the I&A mechanism was found to be inaccessible by all users that are not included in the administrator group. In addition, the I&A information associated with the primary Triad Plus administrator is inaccessible to all other users, including the other administrators.

High Level Discretionary Access Control

The DAC mechanism was found to function properly at the DOS interface. The team found no way to circumvent the mechanism when restricted to standard DOS function calls.

When restricted to standard DOS function calls, the file hiding option was also found to work as stated in the documentation; a user may only obtain evidence of files to which he has access. However, if a user attempts to create an already existing file, whether he has access or not, a DOS error message is generated and the file is not created.

---

(1) The IBM PC/AT was configured with a single floppy disk drive and two fixed hard disk drives.

(2) The IBM PC/XT was configured with a single floppy disk drive and a single fixed hard disk drive.

(3) PC-DOS is a registered trademark of the IBM Corporation.

Low Level Discretionary Access Control

The team found that the DAC mechanism could be bypassed using disk utility programs. However, all files that are inaccessible from DOS are also encrypted in order to provide additional assurance. (The encryption algorithm was not evaluated by the team.) Thus, although the DAC file descriptors could be circumvented, the data retrieved is still in encrypted form.

Resource Access Control

The RAC mechanism was found to function as stated in the documentation; no access to unauthorized resources was permitted, including attempted accesses via direct BIOS calls.

Object Reuse

The object reuse mechanism was found to function as stated in the documentation; RAM is cleared at logoff and, when enabled, files were overwritten when deleted by DOS. This includes deletion by explicit user action (i.e., DOS delete command) or by application programs using DOS calls to delete files.

Audit

The audit records were found to contain the following information: time, date, command, command parameters, and an unused field represented by five zeroes. An audit record is generated at each logon, with the exception of logon attempts during invalid time periods. The record contains user identification information. Since the workstation supports only one concurrent user, all subsequent records are assumed to have been generated by this user until a new logon record is generated. After logging on to the workstation, audit records are created for all DOS programs and attempted security violations. However, audit records are not generated for any built-in DOS commands (e.g., copy, del, mkdir, rmdir, type).

Audit records can be stored in two locations on a workstation equipped with Triad Plus: in a file on either the hard or floppy disk and in a RAM buffer, capable of storing 100 to 200 audit records, on the Triad Plus board. All audit records are placed in the RAM buffer which is periodically flushed to the disk file. It was determined that, once all audit data storage area (i.e., the RAM buffer and the disk) is exhausted, the workstation will no longer be allowed to perform auditable actions. As a result, because logging on is an auditable action, users are no longer allowed to log on. Therefore, no audit data is lost and WA intervention is required.

The previous paragraph does not apply to users who have no access to the disk used for audit data storage. Audit data for these users can only be stored in the RAM buffer on the Triad Plus board. Once this buffer is exhausted, the oldest audit records are overwritten with new ones. This buffer will remain in this condition until a user with access to the audit data storage disk logs on, at which time it will be flushed to that disk.

With the exception of the Triad Plus RAM buffer, the team found that the audit information could be damaged through the use of disk utility programs. However, because the audit data is encrypted, the audit information is protected so that there is some assurance that intelligible changes will not be made.

Controlled Access Mechanism

The mechanism is implemented effectively by the Triad Plus board such that information stored on the board is protected from tampering. The evaluation team found no method of bypassing this mechanism.

XENIX

Although the Triad Plus documentation states that it requires PC DOS, the I&A, Audit, and CAM features were found to operate properly under XENIX. All other Triad Plus features were found to be disabled or unusable in this environment.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION
UNCLASSIFIED

1b. RESTRICTIVE MARKINGS
NONE

2a. SECURITY CLASSIFICATION AUTHORITY

2b. DECLASSIFICATION / DOWNGRADING SCHEDULE

3. DISTRIBUTION / AVAILABILITY OF REPORT
DISTRIBUTION UNLIMITED

4. PERFORMING ORGANIZATION REPORT NUMBER(S)
CSC-EPL-87/006

5. MONITORING ORGANIZATION REPORT NUMBER(S)
S228,557

6a. NAME OF PERFORMING ORGANIZATION
National Computer Security Center

6b. OFFICE SYMBOL *(If applicable)*
C12

7a. NAME OF MONITORING ORGANIZATION

6c. ADDRESS (City, State, and ZIP Code)
9800 Savage Road
Ft. George G. Meade, MD 20755-6000

7b. ADDRESS (City, State, and ZIP Code)

8a. NAME OF FUNDING / SPONSORING ORGANIZATION

8b. OFFICE SYMBOL *(If applicable)*

9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER

8c. ADDRESS (City, State, and ZIP Code)

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO.	TASK NO	WORK UNIT ACCESSION NO

11. TITLE *(Include Security Classification)*
(U) Sub-system Evaluation Report, Micronyx, Inc. Triad Plus, Version 1.3

12. PERSONAL AUTHOR(S)
James L. Arnold, Stephen F. Carlton, Shawn M. Rovansek, John W. Taylor

13a. TYPE OF REPORT
Final

13b. TIME COVERED
FROM ________ TO ________

14. DATE OF REPORT (Year, Month, Day)
870831

15. PAGE COUNT
24

16. SUPPLEMENTARY NOTATION

17. COSATI CODES

FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS *(Continue on reverse if necessary and identify by block number)*
NCSC; TCSEC; sub-system; Micronyx Triad Plus;
I&A; DAC; RAC Object Reuse Audit CAM; Resource Access Control; (KT)

19. ABSTRACT *(Continue on reverse if necessary and identify by block number)*

The Micronyx, Inc. Triad Plus product was evaluated against the I+A identification and authentication DAC, discretionary access control, object reuse and audit requirements detailed in the Department of Defense Trusted Computer System Evaluation Criteria, dated December 1985. The product is an IBM expansion board which, when properly installed, provides trust through the implementation of the security features listed above. The product was found to effectively provide its own state of execution, protecting its own resources from non-administrative workstation users. The product was also found to be essentially transparent to users in the standard DOS environment. This report documents the evaluation of this product.

Keywords: computer security; computer hardware;

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS

21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL
LTC Lloyd D. Gary, USA

22b. TELEPHONE (Include Area Code)
(301) 859-4458

22c. OFFICE SYMBOL
C/C12

Previous editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED